



Wooley, T. D. (2017). A Superpowered Euclidean Prime Generator. *American Mathematical Monthly*, 124(4), 351-352.  
<https://doi.org/10.4169/amer.math.monthly.124.4.351>

Peer reviewed version

License (if available):  
CC BY-NC

Link to published version (if available):  
[10.4169/amer.math.monthly.124.4.351](https://doi.org/10.4169/amer.math.monthly.124.4.351)

[Link to publication record in Explore Bristol Research](#)  
PDF-document

This is the author accepted manuscript (AAM). The final published version (version of record) is available online via MAA at <http://www.maa.org/press/periodicals/american-mathematical-monthly/american-mathematical-monthly-april-2017>. Please refer to any applicable terms of use of the publisher.

## University of Bristol - Explore Bristol Research

### General rights

This document is made available in accordance with publisher policies. Please cite only the published version using the reference above. Full terms of use are available:  
<http://www.bristol.ac.uk/red/research-policy/pure/user-guides/ebr-terms/>

# A Superpowered Euclidean Prime Generator

Trevor D. Wooley

**Abstract.** A variant of Euclid's prime generator is discussed with some of its brethren.

When  $\{\pi_1, \dots, \pi_k\}$  is a finite set of primes, the least divisor exceeding 1 of  $\pi_1 \cdots \pi_k + 1$  is a prime distinct from  $\pi_1, \dots, \pi_k$ . In this way, as every schoolchild knows, one sees that there are infinitely many primes: the assumption that there are just finitely many leads to a contradiction. This is essentially the proof attributed to Euclid, who observed that all primes dividing  $\pi_1 \cdots \pi_k + 1$  are distinct from  $\pi_1, \dots, \pi_k$ . But is *every* prime delivered by iterating this algorithm? To be precise, if we put  $\pi_1 = 2$  and then define

$$\pi_{k+1} = \min \{d > 1 : d \text{ divides } \pi_1 \cdots \pi_k + 1\} \quad (k \geq 1),$$

is it the case that the sequence  $(\pi_k)_{k=1}^\infty$  contains all the primes? The widely held conjecture that the answer is in the affirmative remains open more than half a century after Mullin [3] posed this question. There are, however, variants of Euclid's construction that do yield every prime. Given a set of primes  $\{\pi_1, \dots, \pi_k\}$ , Pomerance [2, §1.1.3] defines  $\pi_{k+1}$  to be the least prime distinct from  $\pi_1, \dots, \pi_k$  that divides a number of the form  $d + 1$  for some divisor  $d$  of  $n = \pi_1 \cdots \pi_k$ . He shows that starting with  $\pi_1 = 2$ , every prime is delivered by this iterative process, and moreover (by extensive computations) that  $\pi_k$  is the  $k$ -th smallest prime for  $k \geq 5$ . Booker [1] instead considers the prime divisors  $p$  of the integers  $d + n/d$ , and shows that at each stage in the iteration, choices for  $d$  and  $p$  may be made so that, taking  $\pi_{k+1} = p$ , every prime is delivered.

The iterative processes of Booker [1] and Pomerance [2] involve some kind of ambiguity, in the latter case involving a choice of the divisor  $d$  of  $n = \pi_1 \cdots \pi_k$ , and in the former case a choice of both  $d$  and the prime divisor of  $d + n/d$ . In this note we present a variant of Euclid's prime generator in which the sequence of primes is determined in order by a single choice of divisor.

**Theorem 1.** *Let  $\pi_1 = 2$ , and when  $k \geq 1$ , define  $\pi_{k+1}$  to be the least divisor exceeding 1 of  $n^{\pi_k} - 1$ , where  $n = \pi_1 \cdots \pi_k$ . Then for each  $k$ , the integer  $\pi_k$  is the  $k$ -th smallest prime.*

This “superpowered” variant of Euclid's prime generator has computational value that can only be described as rather less than nanoscopic. However, it has the merit of succinctly delivering the  $(k + 1)$ -st smallest prime in terms of the  $k$  smallest primes. The proof is immediate from the following lemma, the proof of which is reminiscent of the argument underlying the Pollard  $p - 1$  factorization method (see [2, §5.4], [4]).

**Lemma.** When  $n$  is a positive integer, the least prime divisor of  $n^{\pi_n} - 1$  is the smallest prime not dividing  $n$ .

*Proof.* We may plainly suppose that  $n \geq 2$ , for when  $n = 1$  the desired conclusion is immediate. Let  $p$  be the smallest prime not dividing  $n$ , and let the primes dividing  $n$  be  $\pi_1, \dots, \pi_k$ . Then  $p \leq \pi_1 \cdots \pi_k + 1 \leq n + 1$ , as Euclid could have told us. Moreover, all prime divisors of  $p - 1$  lie in  $\{\pi_1, \dots, \pi_k\}$ , and since  $\pi_i^n \geq 2^n \geq n + 1 \geq p$  for

each  $i$ , we find that  $p - 1$  divides  $(\pi_1 \cdots \pi_k)^n$ , and hence also  $n^n$ . But then, defining the integer  $\lambda$  by writing  $n^n = \lambda(p - 1)$ , and noting that  $p$  does not divide  $n$ , we find from Fermat's Little Theorem that  $n^{n^n} = (n^\lambda)^{p-1} \equiv 1 \pmod{p}$ , which is to say that  $p$  divides  $n^{n^n} - 1$ . ■

The argument just described makes it apparent that less profligate exponents are viable. The conclusion of Theorem 1 remains valid, for example, when  $n^{n^n} - 1$  is replaced by  $n^{n^m} - 1$ , in which  $m = \lceil (\log n)/(\log 2) \rceil$ . In this context, we note also that if  $p_k$  denotes the  $k$ -th smallest prime for each  $k$ , and  $n = p_1 \cdots p_k$ , then the argument of the proof of the lemma shows that *all* primes  $p$  with  $p_{k+1} \leq p < 2p_{k+1}$  divide  $n^{n^n} - 1$ .

A Euclidean disciple even more orthodox than enthusiasts of Theorem 1 might demand a means of obtaining the next prime without knowing a single one of the previous (smaller) primes. Even zero-knowledge demands such as this can be met by a direct consequence of the lemma.

**Theorem 2.** *When  $N$  is a positive integer, the smallest prime exceeding  $N$  is the least divisor exceeding 1 of  $N!^{N!} - 1$ .*

For a proof, simply apply the lemma with  $n = N!$ . We encourage readers to entertain themselves by establishing that for each natural number  $N$ , the smallest prime exceeding  $N$  is the least divisor exceeding 1 of  $N!^{N!} - 1$  (the author is grateful to Andrew Booker and Andrew Granville for pointing out this refinement).

**ACKNOWLEDGMENT.** The author is grateful to the referees for their valuable suggestions and comments.

## REFERENCES

1. A. R. Booker, A variant of the Euclid-Mullin sequence containing every prime, *J. Integer Seq.* **19** (2016) Article 16.6.4, 5 pp.
2. R. Crandall and C. Pomerance, *Prime numbers: a computational perspective*, Second edition, Springer, New York, 2005.
3. A. A. Mullin, Research Problem 8. Recursive function theory, *Bull. Amer. Math. Soc.* **69** (1963) 737.
4. J. M. Pollard, Theorems on factorization and primality testing, *Math. Proc. Cambridge Philos. Soc.* **76** (1974) 521–528.

*School of Mathematics, University of Bristol, University Walk, Clifton, Bristol BS8 1TW, United Kingdom*  
matdw@bristol.ac.uk